# Pass Guaranteed Quiz 2026 Latest Oracle 1z0-1104-25: Valid Oracle Cloud Infrastructure 2025 Security Professional Study Guide



P.S. Free & New 1z0-1104-25 dumps are available on Google Drive shared by ExamDumpsVCE: https://drive.google.com/open?id=1EIN1W_WXrh7j2WvsSIt74A3j5PI9q_8F

Once you start to become diligent and persistent, you will be filled with enthusiasms. Nothing can defeat you as long as you are optimistic. We sincerely hope that our 1z0-1104-25 study materials can become your new purpose. Our 1z0-1104-25 study materials can teach you much practical knowledge, which is beneficial to your career development. In order to survive in the society and realize our own values, learning our 1z0-1104-25 Study Materials is the best way. Never top improving yourself. The society warmly welcomes struggling people.

## Oracle 1z0-1104-25 Exam Syllabus Topics:

| Topic | Details |
|---|---|
| Topic 1 | • OCI Security Introduction: This section of the exam measures the skills of Cloud Security Professionals and covers the basics of security in Oracle Cloud Infrastructure. It introduces the shared security responsibility model, the core principles of security design, and the use of foundational security services to secure deployments on OCI. |
| Topic 2 | • Protecting Data: This section of the exam measures the skills of Cloud Security Professionals and highlights data security practices in OCI. It tests knowledge of using the Key Management Service for encryption keys, managing secrets in the OCI Vault, and applying features of OCI Data Safe to ensure sensitive data remains protected. |
| Topic 3 | • Protecting Infrastructure - Network and Applications: This section of the exam measures the skills of Cloud Security Professionals and covers methods for securing networks and applications on OCI. Topics include network security groups, firewalls, and security lists, while also focusing on the use of load balancers for availability. The section further addresses the configuration of OCI certificates and web application firewalls to strengthen infrastructure security. |
| Topic 4 | • Implementing Identity and Access Management (IAM): This section of the exam measures skills of OCI Administrators and focuses on identity and access controls. It covers IAM domains, users, groups, and compartments, as well as the use of IAM policies to manage access to resources. Candidates are also tested on configuring dynamic groups, network sources, and tag-based access control, along with managing MFA, sign-on policies, and activity monitoring. |

# 1z0-1104-25 Prep Torrent - 1z0-1104-25 Latest Questions & 1z0-1104-25 Vce Guide

Many customers want to check the content and quality of our 1z0-1104-25 exam braindumps. So we develped trial versions for you. After you have used a trial version, you will have an overview of the content of the 1z0-1104-25 simulating exam. This is enough to convince you that this is a product with high quality. If you are sure that you want this product, but we are not sure which version to buy, we can let you try multiple versions of 1z0-1104-25 learning guide. And there are three varied versions on our website.

## Oracle Cloud Infrastructure 2025 Security Professional Sample Questions (Q20-Q25):

**NEW QUESTION # 20**
"A company, ABC, is planning to launch a new web application on OCI. Based on past experiences, they expect a significant surge in traffic after the launch. You are responsible for ensuring that the application is highly available.
Which step would you perform to achieve this goal?

- A. Configure Cloud Guard to prevent large amounts of traffic from reaching the web application.
- B. Use a Virtual Cloud Network (VCN) with subnets, security lists, and routing rules to isolate the web application from the Internet and other resources.
- C. Implement security controls, such as web application firewalls, to protect against common attack vectors.
- D. Use a load balancer to distribute incoming traffic evenly across multiple instances of the web application."

**Answer: D**

**NEW QUESTION # 21**
Task 6: Create Load Balancer and Attach Certificate
Create a Load Balancer with the name PBT-CERT-LB-01 in subnet LB-Subnet-PBT-CERT-SNET-02 Create a Listener for the load balancer, where:
Name: PBT-CERT-LB_LTSN_01
Protocol: HTTPS
Port: 443
Attach the certificate PBT-CERT-01-<username> to the load balancer
Attach the security list PBT-CERT-LB-SL-01 to subnet LB-Subnet-PBT-CERT-SNET-02 See the solution below in Explanation.

**Answer:**

Explanation:
Task 6: Create Load Balancer and Attach Certificate
Step 1: Create the Load Balancer
* Log in to the OCI Console.
* Navigate to Networking>Load Balancers.
* Click Create Load Balancer.
* Enter the following details:
* Name: PBT-CERT-LB-01
* Compartment: Select your assigned compartment.
* Load Balancer Type: Select Public.
* Virtual Cloud Network: Select PBT-CERT-VCN-01.
* Subnet: Select LB-Subnet-PBT-CERT-SNET-02.
* Shape: Choose a shape (e.g., 10 Mbps, adjust based on needs).
* Click Next.
* Leave backend sets and listeners as default for now (we'll configure the listener next).
* Click Create Load Balancer and wait for it to be provisioned.
Step 2: Create a Listener

* Once the load balancer is created, go to theLoad Balancerspage and click on PBT-CERT-LB-01.
* UnderResources, clickListeners.
* ClickCreate Listener.
* Enter the following details:
* Name: PBT-CERT-LB_LTSN_01
* Protocol: SelectHTTPS.
* Port: Enter 443.
* Certificate: ClickAdd Certificate, then select the PBT-CERT-01<username> certificate (e.g., PBT-CERT-0199008677labuser01) created in Task 5.
* Leave other settings (e.g., SSL handling) as default unless specified.
* ClickCreate.
Step 3: Configure the Backend Set
* In the PBT-CERT-LB-01 details page, underResources, clickBackend Sets.
* ClickCreate Backend Set(if not already created).
* Enter basic details (e.g., name like PBT-CERT-BS-01).
* Add a backend server:
* IP Address: Use the private IP of PBT-CERT-VM-01 (find this in the instance details under Compute>Instances).
* Port: 80 (HTTP, as configured on the web server).
* Protocol: HTTP.
* ClickCreate.
Step 4: Attach the Security List to the Subnet
* Navigate toNetworking>Virtual Cloud Networks.
* Select PBT-CERT-VCN-01 and clickSubnets.
* Click on LB-Subnet-PBT-CERT-SNET-02.
* UnderSecurity Lists, ensure PBT-CERT-LB-SL-01 is attached. If not:
* ClickEdit.
* Remove the default security list and add PBT-CERT-LB-SL-01.
* ClickSave Changes.
Step 5: Verify the Configuration
* Ensure the load balancer health status is OK (check underBackend Sets>Health).
* Test by accessing https://<load-balancer-public-ip> in a browser (replace with the public IP from the load balancer details).

## NEW QUESTION # 22

You are a security architect at your organization and have noticed an increase in cyberattacks on your applications, including Cross-Site Scripting (XSS) and SQL Injection. To mitigate these threats, you decide to use OCI Web Application Firewall (WAF). Which type of OCI WAF rule should you configure to protect against these attacks?

- A. Access control rule
- B. Protection rule
- C. Rate Limiting rule
- D. Encryption rule

**Answer: B**

## NEW QUESTION # 23

Within OCI IAM identity domains, the AD Bridge component serves a critical role. How does the AD Bridge functionality specifically enhance Identity and Access Management (IAM) practices?

- A. It simplifies user provisioning by enabling automated synchronization of user accounts and group memberships from an existing Microsoft Active Directory (AD) environment.
- B. It strengthens access security by providing an additional layer of authentication through AD integration.
- C. It directly integrates with OCI MFA providers, allowing for seamless enforcement of MFA for users authenticated through AD credentials.
- D. It facilitates delegated administration, allowing authorized AD users to manage specific resources within the OCI identity domain.

**Answer: A**

## NEW QUESTION # 24

During your investigation of a load balancer issue, you discovered that all back-end servers associated with one of the affected listeners were reported as unhealthy. However, when you checked the back-end servers, they seemed to be working just fine. What might be causing this issue?

- A. Misconfigured health check
- B. Incorrect DNS configuration
- C. Incorrect subnet configuration
- D. Overloaded back-end servers
- E. Misconfigured security rule

**Answer: A**


## NEW QUESTION # 25

......